What is claimed is:

CLAIMS

1. A method for producing at least one ciphertext block from at least one plaintext block using a block cipher *E* and a key *K*, the method comprising:

receiving n plaintext blocks, wherein n is an integer greater than 0;

setting Q_0 equal to an initial value; and

for each plaintext block of the n plaintext blocks:

computing $Q_i = E_K(Q_{i-1})\ XOR\ P_i$; and

computing $C_i = M(P_i, Q_i)$,

thereby producing n ciphertext blocks,

wherein:

$0 < i <= n$, and

P_i denotes an i - th plaintext block of the n plaintext blocks, and

C_i denotes an i - th ciphertext block of the n ciphertext blocks, and

M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of *M* if bit P_{ij} is not to be encrypted, and selects a second argument of *M* if bit P_{ij} is to be encrypted.

2. The method according to claim 1 and wherein M is chosen in accordance with a standard indicating bits that are not to be encrypted.

3. The method according to claim 2 and wherein the standard comprises one of the following: an audio standard; a video standard; and an audio-video standard.

4. The method according to claim 3 and wherein the standard comprises MPEG-2.

5. A method for producing at least one ciphertext block from at least one plaintext block using a block cipher E and a key K, the method comprising:

receiving n plaintext blocks, wherein n is an integer greater than 0, and an initial value IV;

computing $IV' = M(P_1, IV)$;

computing $Q_0 = H(IV')$; and

for each plaintext block of the n plaintext blocks:

computing $Q_i = E_K(Q_{i-1})$ XOR P_i; and

computing $C_i = M(P_i, Q_i)$,

thereby producing n ciphertext blocks,

wherein:

$0 < i <= n$, and

H is a hash function, and

P_i denotes an i - th plaintext block of the n plaintext blocks, and

C_i denotes an i - th ciphertext block of the n ciphertext blocks, and

M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of M if bit P_{ij} is not to be encrypted, and selects a second argument of M if bit P_{ij} is to be encrypted.

6. The method according to claim 5 and wherein H comprises SHA1.

7. The method according to claim 5 and wherein $H(IV')$ comprises $E_K(IV')$ XOR IV'.

8. The method according to any of claims 5 - 7 and wherein M is chosen in accordance with a standard indicating bits that are not to be encrypted.

9. The method according to claim 8 and wherein the standard comprises one of the following: an audio standard; a video standard; and an audio-video standard.

10. The method according to claim 9 and wherein the standard comprises MPEG-2.

11. In a method for producing at least one ciphertext block from at least one plaintext block using a block cipher *E* and a key *K* in a stream mode, wherein P_i denotes an i - th plaintext block, and C_i denotes an i - th ciphertext block, an improvement comprising:

for each bit C_{ij} of block C_i, selecting P_{ij} as an output if bit P_{ij} is not to be encrypted.

12. The method according to claim 11 and wherein the stream mode comprises CFM mode.

13. Apparatus for producing at least one ciphertext block from at least one plaintext block using a block cipher *E* and a key *K*, the at least one plaintext block comprising n plaintext blocks, the at least one ciphertext block comprising n ciphertext blocks, wherein n is an integer greater than 0, the apparatus comprising:

an initialization unit for setting Q_0 equal to an initial value; and

a computation unit operative, for each plaintext block of the n plaintext blocks:

to compute $Q_i = E_K(Q_{i-1})\ XOR\ P_i$; and

to compute $C_i = M(P_i, Q_i)$,

wherein:

$0 < i <= n$, and

P_i denotes an i - th plaintext block of the n plaintext blocks, and

C_i denotes an i - th ciphertext block of the n ciphertext blocks, and

M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of M if bit P_{ij} is not to be encrypted, and selects a second argument of M if bit P_{ij} is to be encrypted.

14. Apparatus for producing at least one ciphertext block from at least one plaintext block using a block cipher *E*, a key *K*, and an initial value *IV*, the at least one plaintext block comprising n plaintext blocks, the at least one ciphertext block comprising n ciphertext blocks, wherein n is an integer greater than 0, the apparatus comprising:

a first computation unit for computing $IV' = M(P_1, IV)$;

a second computation unit for computing $Q_0 = H(IV')$; and

a third computation unit operative, for each plaintext block of the n plaintext blocks:

to compute $Q_i = E_K(Q_{i-1})\ XOR\ P_i$; and

to compute $C_i = M(P_i, Q_i)$,

wherein:

$0 < i <= n$, and

H is a hash function, and

P_i denotes an i - th plaintext block of the n plaintext blocks, and

C_i denotes an i - th ciphertext block of the n ciphertext blocks, and

M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of M if bit P_{ij} is not to be encrypted, and selects a second argument of M if bit P_{ij} is to be encrypted.

15. In apparatus for producing at least one ciphertext block from at least one plaintext block using a block cipher E and a key K in a stream mode, wherein P_i denotes an i - th plaintext block, and C_i denotes an i - th ciphertext block, an improvement comprising:

a selector unit operative, for each bit C_{ij} of block C_i, to select P_{ij} as an output if bit P_{ij} is not to be encrypted.

16. A method for producing at least one plaintext block from at least one ciphertext block encrypted using a block cipher E and a key K, the method comprising:

receiving n ciphertext blocks, where n is an integer greater than 0;

setting Q_0 equal to an initial value; and

for each ciphertext block of the n ciphertext blocks:

computing $Q'_i = E_K(Q_{i-1})\ XOR\ C_i$;

computing $P_i = M(C_i\ ,\ Q'_i)$; and

computing $Q_i = M(Q'_i\ ,\ C_i)$,

thereby producing n plaintext blocks,

wherein:

$0 < i <= n$, and

P_i denotes an i - th plaintext block of the n plaintext blocks, and

C_i denotes an i - th ciphertext block of the n ciphertext blocks, and

M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of *M* if bit P_{ij} is not encrypted, and selects a second argument of *M* if bit P_{ij} is encrypted.

17. The method according to claim 16 and wherein *M* is chosen in accordance with a standard indicating bits that are not encrypted.

18. The method according to claim 17 and wherein the standard comprises one of the following: an audio standard; a video standard; and an audio-video standard.

19. The method according to claim 18 and wherein the standard comprises MPEG-2.

20. A method for producing at least one plaintext block from at least one ciphertext block using a block cipher *E* and a key *K*, the method comprising:

receiving n ciphertext blocks, wherein n is an integer greater than 0, and an initial value *IV*;

computing $IV' = M(P_1, IV)$;

computing $Q_0 = H(IV')$; and

for each ciphertext block of the n ciphertext blocks:

computing $Q'_i = E_K(Q_{i-1})\ XOR\ C_i$;

computing $P_i = M(C_i, Q'_i)$; and

computing $Q_i = M(Q'_i, C_i)$,

thereby producing n plaintext blocks,

wherein:

$0 < i <= n$, and

H is a hash function, and

P_i denotes an i - th plaintext block of the n plaintext blocks, and

C_i denotes an i - th ciphertext block of the n ciphertext blocks, and

M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of M if bit P_{ij} is not encrypted, and selects a second argument of M if bit P_{ij} is encrypted.

21. The method according to claim 20 and wherein H comprises SHA1.

22. The method according to claim 20 and wherein $H(IV')$ comprises $E_K(IV')\ XOR\ IV'$.

23. The method according to any of claims 20 - 22 and wherein M is chosen in accordance with a standard indicating bits that are not encrypted.

24. The method according to claim 23 and wherein the standard comprises one of the following: an audio standard; a video standard; and an audio-video standard.

25. The method according to claim 24 and wherein the standard comprises MPEG-2.

26. In a method for producing at least one plaintext block from at least one ciphertext block using a block cipher *E* and a key *K* in a stream mode, wherein P_i denotes an i - th plaintext block of the plurality of plaintext blocks, and C_i denotes an i - th ciphertext block of the plurality of ciphertext blocks, an improvement comprising:

for each bit P_{ij} of block P_i, selecting C_{ij} as an output if bit C_{ij} is not encrypted.

27. The method according to claim 26 and wherein the stream mode comprises CFM mode.

28. Apparatus for producing at least one plaintext block from at least one ciphertext block encrypted using a block cipher *E* and a key *K*, the at least one ciphertext block comprising n ciphertext blocks, the at least one plaintext block comprising n plaintext blocks, wherein n is an integer greater than 0, the apparatus comprising:

initialization apparatus for setting Q_0 equal to an initial value; and

a computation unit operative, for each ciphertext block of the n ciphertext blocks:

to compute $Q'_i = E_K(Q_{i-1})\ XOR\ C_i$;

to compute $P_i = M(C_i , Q'_i)$; and

to compute $Q_i = M(Q'_i , C_i)$,

wherein:

$0 < i <= n$, and

P_i denotes an i - th plaintext block of the n plaintext blocks, and

C_i denotes an i - th ciphertext block of the n ciphertext blocks, and

M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of M if bit P_{ij} is not encrypted, and selects a second argument of M if bit P_{ij} is encrypted.

29. Apparatus for producing at least one plaintext block from at least one ciphertext block using a block cipher E and a key K, the at least one ciphertext block comprising n ciphertext blocks, the at least one plaintext block comprising n plaintext blocks, wherein n is an integer greater than 0, the apparatus comprising:

a first computation unit for computing $IV' = M(P_1 , IV)$;

a second computation unit for computing $Q_0 = H(IV')$; and

a third computation unit operative, for each ciphertext block of the n ciphertext blocks:

to compute $Q'_i = E_K(Q_{i-1})$ XOR C_i;

to compute $P_i = M(C_i, Q'_i)$; and

to compute $Q_i = M(Q'_i, C_i)$,

wherein:

$0 < i <= n$, and

H is a hash function, and

P_i denotes an i - th plaintext block of the n plaintext blocks, and

C_i denotes an i - th ciphertext block of the n ciphertext blocks, and

M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of M if bit P_{ij} is *not* encrypted, and selects a second argument of M if bit P_{ij} is encrypted.

30. In apparatus for producing at least one plaintext block from at least one ciphertext block using a block cipher E and a key K in a stream mode, wherein P_i denotes an i - th plaintext block of the plurality of plaintext blocks, and C_i denotes an i - th ciphertext block of the plurality of ciphertext blocks, an improvement comprising:

a selector unit operative, for each bit P_{ij} of block P_i, to select C_{ij} as an output if bit C_{ij} is not encrypted.